

PANORAMICA DELLA
SOLUZIONE



LIVEGUARD ADVANCED

**Difesa proattiva contro tipi di minacce
zero-day e mai viste prima.**

Progress. Protected.

Cos'è una **protezione avanzata dalle minacce**

Una tecnologia proattiva basata sul cloud che dispone di scansione adattiva avanzata, machine learning all'avanguardia, sandboxing basato su cloud e analisi comportamentale approfondita per prevenire gli attacchi mirati e i nuovi tipi di minacce mai visti prima, specialmente ransomware.

ESET LiveGuard Advanced fornisce un ulteriore livello di sicurezza per i prodotti ESET come Mail Security, Endpoint e Cloud Office Security. La sua avanzata tecnologia basata su cloud è costituita da diversi tipi di sensori che si aggiungono all'analisi statistica del codice, a un'ispezione dettagliata del campione attraverso il machine learning, alla verifica della memoria e alla rivelazione basata sul comportamento.

Perché utilizzare una difesa proattiva dalle minacce basata sul cloud?

RANSOMWARE

Il Ransomware continua a rappresentare una delle principali minacce per le organizzazioni di tutto il mondo sin dai tempi di Cryptolocker nel 2013. Nonostante il Ransomware esista da molto più tempo, non è mai stato considerato un vero pericolo per le aziende. Tuttavia, oggi un singolo attacco di ransomware può facilmente compromettere l'operatività di un'azienda criptando file importanti o essenziali. Quando un'azienda subisce un attacco ransomware, si rende immediatamente conto che i backup di cui dispone non sono abbastanza recenti, e si sente quasi obbligata a pagare il riscatto.

Una soluzione proattiva di rilevamento delle minacce basata su cloud fornisce un ulteriore livello di difesa al di fuori della rete aziendale per evitare che il ransomware venga eseguito in un ambiente di produzione.

OBIETTIVI MIRATI E VIOLAZIONE DEI DATI

L'attuale panorama della sicurezza informatica è in costante evoluzione con nuovi metodi di attacco e minacce mai viste prima d'ora. Quando si verifica un attacco o una violazione di dati, le aziende sono in genere sorprese che le loro difese siano state compromesse o sono completamente inconsapevoli dell'avvenuto attacco. Una volta scoperto, le aziende mettono prontamente in atto delle misure di protezione per evitare che si ripeta. Tuttavia, questo non li protegge da un attacco successivo che potrebbe utilizzare un diverso e nuovo vettore.

L'approccio di una security sandbox basata su cloud è molto più efficace rispetto a una semplice osservazione della potenziale minaccia, perché va oltre la semplice apparenza e ne analizza anche il comportamento. Questo permette di essere molto più decisivi nel determinare se si tratta di un attacco mirato, una minaccia persistente o di nulla di pericoloso.

L'analisi statica e dinamica viene eseguita da una serie di algoritmi di apprendimento automatico, utilizzando tecniche che includono il deep learning.

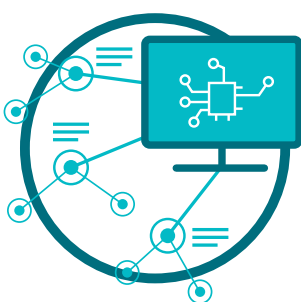
Una security sandbox basata su cloud al di fuori della rete dell'utente può andare oltre la semplice analisi dell'aspetto, osservando invece ciò che la potenziale minaccia fa effettivamente.

I nostri prodotti e le nostre tecnologie poggiano su 3 pilastri



ESET LIVEGRID®

Quando una minaccia zero-day come un ransomware viene intercettata, il file viene inviato al nostro sistema di protezione malware su Cloud – ESET LiveGrid®- dove viene eseguito per controllarne il comportamento. I risultati vengono condivisi in tempo reale con tutti gli endpoint a livello globale senza dover attendere alcun aggiornamento.



MACHINE LEARNING

Usa il potere combinato di reti neurali e di algoritmi scelti con cura per stabilire se un campione è da considerarsi innocuo, potenzialmente indesiderato o pericoloso.



ESPERIENZA UMANA

I migliori ricercatori di sicurezza informatica di tutto il mondo condividono il proprio know-how e le proprie analisi per garantire la condivisione di minacce note 24 ore su 24.



ESET fa la differenza

PROTEZIONE MULTILIVELLO

ESET LiveGuard Advanced è una soluzione di difesa dalle minacce basata sul cloud che esegue tutti i campioni sospetti che vengono inviati in un ambiente di test sicuro presso la sede centrale di ESET, dove il loro comportamento viene valutato utilizzando i feed delle informazioni sulle minacce, i molteplici strumenti interni di ESET per l'analisi statica e dinamica e i dati sulla reputazione in modo da rilevare le minacce zero-day. Per analizzare i campioni vengono utilizzati quattro strati, che possono essere distribuiti dinamicamente in base ai risultati emersi. ESET LiveGuard Advanced combina tutti i risultati dei livelli di rilevamento e valuta lo stato di ogni campione. I risultati vengono trasmessi prima al prodotto di sicurezza ESET dell'utente e poi all'infrastruttura della sua azienda.

VISIBILITÀ COMPLETA

Per ogni campione analizzato, è possibile visualizzare il risultato nella console di ESET PROTECT. Inoltre i clienti con una licenza con più di 100 postazioni ricevono un rapporto comportamentale completo con informazioni dettagliate sui campioni e sul loro comportamento osservato durante l'analisi nella sandbox. Tutte le informazioni vengono mostrate in maniera chiara e comprensibile. Non ci limitiamo a mostrare i campioni inviati a ESET LiveGuard Advanced ma anche tutto ciò che viene inviato a ESET's Cloud Malware Protection System - ESET LiveGrid®.

MOBILITÀ

Al giorno d'oggi, i dipendenti aziendali lavorano sempre più spesso in remoto e non in sede. Ecco perché ESET LiveGuard Advanced può analizzare i file indipendentemente da dove si trovano gli utenti. La cosa più interessante è che se vengono individuate delle minacce, l'intera azienda viene immediatamente protetta.

PRIVACY

ESET prende molto sul serio il rispetto della privacy. Attraverso impostazioni specifiche, l'utente può richiedere a ESET di cancellare i campioni subito dopo l'analisi.

VELOCITÀ SENZA PARI

Ogni singolo minuto è importante. Per questo motivo, ESET LiveGuard Advanced è progettato per analizzare la maggior parte dei campioni in meno di 5 minuti. Se i campioni erano già stati analizzati in precedenza, avrà bisogno di pochi secondi per garantire protezione a tutti i dispositivi della vostra azienda.

COLLAUDATO E AFFIDABILE

ESET opera nel settore della sicurezza da oltre 30 anni e continuiamo ad evolvere la nostra tecnologia per essere sempre un passo avanti rispetto alle nuove minacce. Come risultato, 1 miliardo di utenti internet in tutto il mondo sono ora protetti da ESET. La nostra tecnologia è costantemente esaminata e provata da test di organizzazioni indipendenti che dimostrano quanto sia efficace il nostro approccio per fermare le minacce più recenti.

DIFESA PROATTIVA

Se viene rilevato un campione sospetto, ne viene bloccata l'esecuzione, in attesa dell'analisi di ESET LiveGuard Advanced. Questo impedisce alle potenziali minacce di portare scompiglio nel sistema dell'utente. Inoltre, una volta completata l'analisi, se viene rilevata una minaccia su un endpoint, l'informazione viene comunicata in pochi minuti a tutti gli endpoint della rete dell'organizzazione, proteggendo immediatamente qualsiasi utente potenzialmente a rischio.

Casi pratici

Ransomware

CASI PRATICI

Il Ransomware si diffonde solitamente nelle caselle di posta elettronica di utenti ignari.

SOLUZIONE

- ✓ ESET Mail Security invia automaticamente gli allegati sospetti delle email a ESET LiveGuard Advanced.
- ✓ ESET LiveGuard Advanced analizza il campione, quindi invia il risultato a Mail Security solitamente entro 5 minuti.
- ✓ ESET Mail Security rileva e filtra automaticamente gli allegati che contengono contenuti dannosi.
- ✓ L'allegato dannoso non raggiunge mai il destinatario.

Protezione granulare per i diversi ruoli aziendali

CASI PRATICI

Ogni ruolo in azienda richiede diversi livelli di protezione. Gli sviluppatori o il personale IT necessitano di restrizioni di sicurezza diverse rispetto al responsabile dell'ufficio o al CEO.

SOLUZIONE

- ✓ Configurare un criterio unico per computer o per server in ESET LiveGuard Advanced.
- ✓ Applicare automaticamente un criterio differente basato su un diverso gruppo di utenti statici o gruppo di Active Directory.
- ✓ Cambiare automaticamente le impostazioni di configurazione semplicemente spostando un utente da un gruppo a un altro.



File sconosciuti o sospetti

CASI PRATICI

A volte i dipendenti o il personale IT potrebbero ricevere un file che vogliono sottoporre a una doppia verifica.

SOLUZIONE

- ✓ Ogni utente può inviare un campione da analizzare direttamente da tutti i prodotti ESET.
- ✓ Il campione viene analizzato rapidamente da ESET LiveGuard Advanced.
- ✓ Se un file è ritenuto dannoso, tutti i computer dell'azienda sono protetti.
- ✓ L'amministratore IT ha piena visibilità sull'utente che ha inviato il campione e sull'esito, negativo o positivo, dell'analisi.



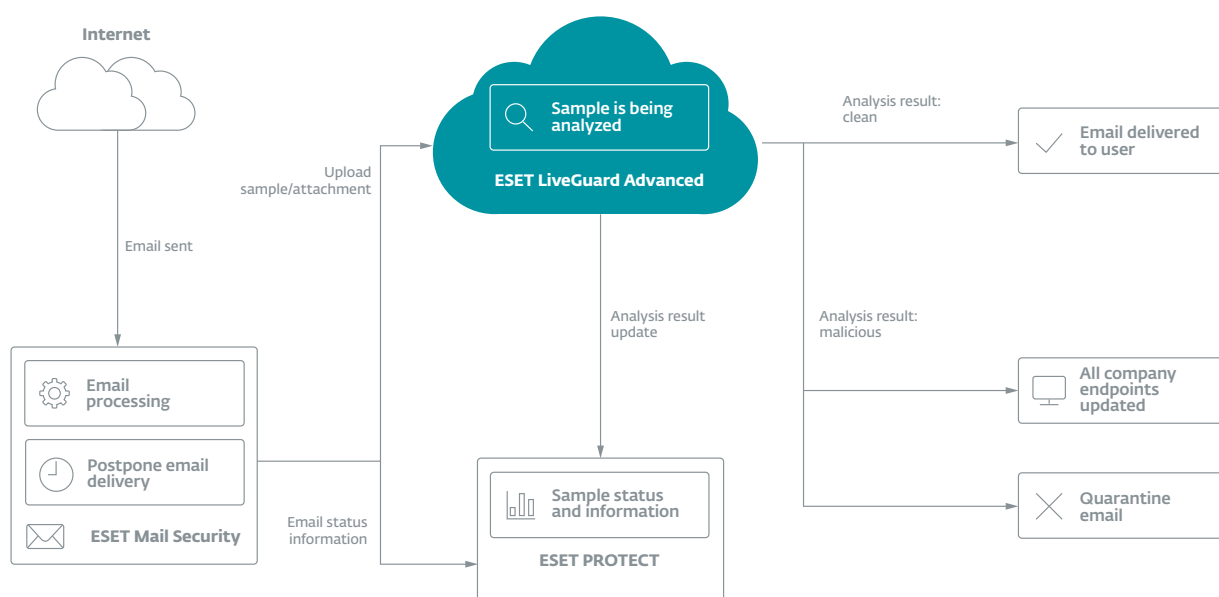
The screenshot displays the ESET LiveGuard Advanced interface with the following sections:

- VERY SUSPICIOUS**: A red banner with a warning icon and a file hash: `5E7CA83DC41DC100F9F8A93009E1248B2AF6DC`. It indicates the sample is suspicious.
- ADVANCED SCANNING ENGINES**:
 - Advanced Unpacking And Scanning**: A red banner with a warning icon, stating the sample was unpacked and analyzed against an enriched threat database. Sample is malicious.
 - Advanced Machine Learning Detection**: A green banner with a checkmark, stating a static and dynamic analysis was performed by an array of machine learning algorithms, including deep learning. Sample is clean.
- BEHAVIORAL ANALYSIS SANDBOX**:
 - Experimental Sandbox Engine**: An orange banner with an information icon, stating a sample was executed in a sandbox environment. Sample is suspicious.
 - In-Depth Behavioral Analysis**: A red banner with a warning icon, stating memory dumps produced by previous ESET scans are subject to an in-depth behavioral analysis that identifies known malicious patterns and chains of actions. Sample is malicious.
- ANALYZED BEHAVIORS**: A table listing detected behaviors:

Behavior	Status
Anti-Debug Trick	Behaviour not detected
Anti-Debug Trick	Behaviour not detected
Anti-Debug Trick	Behaviour not detected

Come funziona ESET LiveGuard Advanced

Con ESET Mail Security



ESET LiveGuard Advanced è compatibile con i prodotti ESET Endpoint, Server e Cloud app security (Microsoft 365), ed è completamente integrato nelle console di gestione ESET.

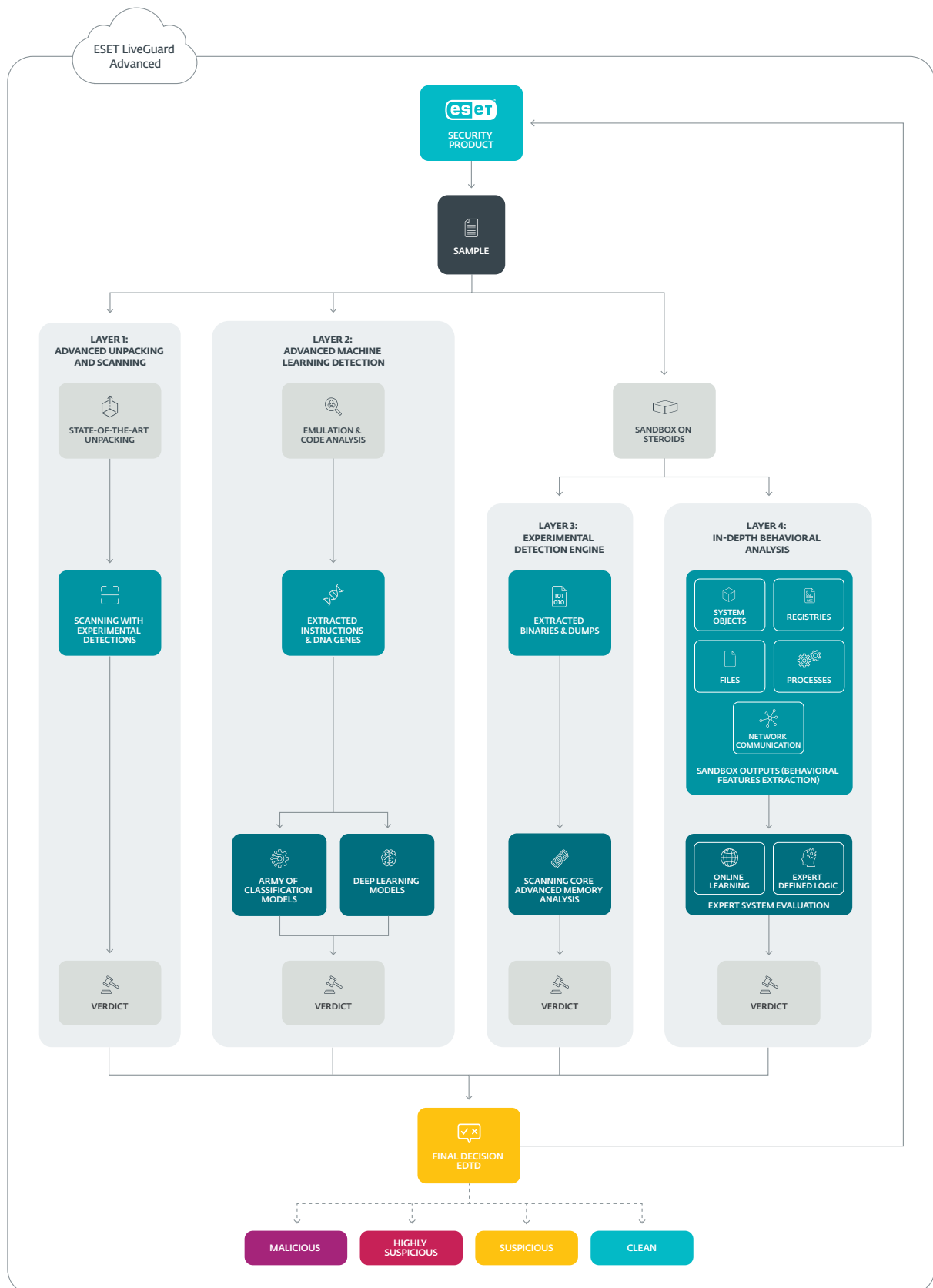
"Prodotto Incredibile!"

Cosa ti piace di più?

"Mi piace la facilità con cui è stato implementato su tutte le mie postazioni di lavoro e la rapidità con cui ha messo in sicurezza la rete. Ho rilevato un software indesiderato e vedo quotidianamente email che impediscono ai bug di rete di diventare un problema. Dormo meglio sapendo che la mia rete è protetta da ESET".

- Michael P. / Network manager / Media Impresa (51-1.000 dipendenti).

Come funziona la nostra analisi avanzata



ESET LiveGuard Advanced utilizza 4 livelli distinti di rilevamento per garantire la massima efficacia. Ogni livello utilizza un approccio diverso e fornisce un verdetto sul campione. La valutazione finale comprende i risultati di tutte le informazioni sul campione.

LIVELLO 1

Decompressione e controllo avanzati

I campioni vengono sottoposti ad un'analisi statica e ad una decompressione avanzata e vengono poi confrontati con un database delle minacce aggiornato.

LIVELLO 2

Rilevamento apprendimento automatico avanzato

L'analisi statica e dinamica viene eseguita da una serie di algoritmi di apprendimento automatico, utilizzando tecniche che includono il deep learning.

LIVELLO 3

Motore di rilevamento sperimentale

I campioni sono inseriti in una sorta di "sandbox su steroidi" che assomigliano molto ai dispositivi utente su scala reale. Successivamente, vengono monitorati per individuare eventuali segni di comportamento dannoso.

LIVELLO 4

Analisi del comportamento approfondita

Tutti gli output della sandbox sono sottoposti a un'analisi comportamentale approfondita che identifica azioni dannose o sospette.

ESET LIVEGUARD ADVANCED COMBINA TUTTI I RISULTATI EMERSI DAI LIVELLI DI RILEVAMENTO E VALUTA LO STATO DEL CAMPIONE. I RISULTATI VENGONO TRASMESSI PRIMA AL PRODOTTO DI SICUREZZA ESET DELL'UTENTE E POI ALL'INFRASTRUTTURA DELLA SUA AZIENDA.

VELOCITÀ INCOMPARABILE



Il Sandbox dedicato compie l'analisi in meno di 5 minuti

RISPARMIO DI TEMPO



ESET LiveGuard ON



ESET LiveGuard OFF

+ 135min

ti tempo guadagnato

Informazioni su ESET

Per oltre 30 anni, ESET® ha sviluppato software e servizi di sicurezza IT tra i migliori del settore, offrendo soluzioni di protezione complete e multistrato contro le minacce di cybersecurity per aziende e consumatori di tutto il mondo. ESET è da tempo all'avanguardia

nello sviluppo di tecnologie di machine learning e cloud che prevengono, rilevano e reagiscono al malware. ESET è un'azienda privata che promuove la ricerca e lo sviluppo scientifico in tutto il mondo.

ESET IN NUMERI

1bn+
utenti internet
protetti

400k+
clienti
aziendali

**Oltre
200**
paesi e
territori

13
centri R&D
globali

ALCUNI DEI NOSTRI CLIENTI



protetti da ESET dal
2017 più di 9,000
endpoint



protetti da ESET dal
2016 più di 4.000
mailbox



Canon Marketing Japan Group

protetti da ESET dal
2016 più di 32,000
endpoint



Partner di sicurezza
ISP dal 2008 2
milioni di customer
base

IMPEGNATI A MANTENERE I PIÙ ALTI STANDARD DEL SETTORE



ESET ha ricevuto il premio
Business Security APPROVED
da AV - Comparatives nel test di
sicurezza aziendale nel dicembre
2021.



ESET raggiunge costantemente le
prime posizioni nella piattaforma
globale di recensioni G2 e le sue
soluzioni sono apprezzate dai
clienti di tutto il mondo.



Le soluzioni di ESET sono
regolarmente riconosciute dalle
principali società di analisi, tra
cui "The Forrester Tech Tide(TM):
Zero Trust Threat Detection And
Response, Q2 2021" come fornitore
modello.